REMARKS

This application has been carefully reviewed in light of the Office Action dated February 1, 2007. Claims 1, 3 to 5 and 7 to 27 are in the application, of which Claims 1, 22, 23 and 27 are still the only independent claims. Reconsideration and further examination are respectfully requested.

Applicants thank the Examiner for his withdrawal of all prior objections and rejections.

A new rejection was entered for all claims, under 35 U.S.C. § 103(a), over U.S. Patent No. 7,020,773 (Otway) in view of U.S. Patent No. 7,062,651 (Lapstun). In response, Claim 2 has been canceled, and the substance thereof incorporated into independent Claims 1, 22 and 27. Independent Claim 23 has not been amended. Accordingly, this should be viewed as a traversal of the rejection, as detailed more fully below.

Moreover, even though the rejection was marked "final", entry of the above amendments should be allowed. Specifically, the amendments incorporate the substance of now-canceled Claim 2, which has already received the Examiner's full consideration. Accordingly, entry of the amendment would not raise any significant new issues, nor would it require any extensive additional searching. Thus, entry of the amendment is respectfully requested.

Turning to the technological substance of the rejection, the invention concerns secure storage of a public key for encryption of data in a computing device that includes a user-specific key pair that is securely stored in the computing device. In

particular, a user-specific key pair is stored in a secure registry. A public key is received from a printer and a digital signature is created for the public key while using the user-specific key pair. The digital signature created by using the user-specific key pair is verified, and specifically is verified responsive to a printing instruction.

According to one feature of the invention set out in independent Claims 1, 22 and 27, the user-specific key pair is obtained from a key function call which is supported by an operating system executing in the computing device. Thus, in one representative embodiment of the invention described beginning at line 22 of page 15, a Microsoft Windows operating system includes a cryptographic application programming interface (CAPI). A function call is supported by CAPI to retrieve a user-specific key pair for an authorized user. See page 16, lines 9-11. Such an arrangement provides an advantageous effect relative to prior art applications such as PGP ("Pretty Good Privacy"), as described beginning at page 16, line 16. Specifically, such prior art applications are seen to have a significant shortcoming with respect to CAPI functionality or other functionality that is built into the operating system. These prior art applications require the user of the application to maintain the storage of the key pair that is used to create the cryptographic signature. Accordingly, such applications do not maintain the key pair under strict security and may be more prone to a security breach in which an unauthorized user of the computer can access the key pair and use it to access encrypted data of the authorized user.

In entering the rejection of now-canceled Claim 2, the Office Action took the position that Otway describes a user-specific key pair that is obtained from a key function call supported by an operating system executing in Otway's computing device.

See, Office Action, pages 8 and 9, which cite to Otway's Fig. 1 and lines 40-67 of Otway's column 1. Applicants have reviewed the cited portions of Otway, and find absolutely no disclosure or suggestion of the subject matter attributed by the Office Action to these cited portions of Otway. Withdrawal of the rejection on this basis is therefore respectfully requested.

The Office Action (page 9) further took the position that "these features have been admitted per applicant to have been conventional and well known to digital rights management systems at the time the invention was made." Regardless of any alleged admissions, even if these features were well known and conventional (which is not conceded), the Office Action still fails to set out a *prima facie* case of obviousness. In particular, the Office Action fails to articulate any reason that might have prompted one of ordinary skill in the art to combine these elements in the manner set out in the claims herein. More precisely, although it might be true that the Office Action has articulated a rationale for combining Otway and Lapstun, the Office Action does not articulate any rationale whatsoever, for modifying the combined teachings of Otway and Lapstun in the manner set out at pages 8 and 9 of the Office Action.

It is therefore respectfully submitted that at least Claims 1, 22 and 27 are fully in condition for allowance.

With respect to independent Claim 23, which has not been amended, this claim specifies a second receiving step of receiving a printer hash key obtained from a "test page" printed by the printer. This hash key is input into the computing device by a user-input means connected to the computing device.

As described in the specification in terms of preferred embodiments of the invention, such an arrangement provides an advantageous effect in that it is ordinarily possible for the user himself to authenticate the printer key. See, for example, lines 9 through 19 on page 10 of the application as filed. Thus, the authenticity of the printer key is easily verified upon receipt, ordinarily without the need for an external digital certificate or a certification authority.

The Office Action cited to column 3, lines 1 to 30, and column 5, lines 20 to 60, of Otway as allegedly disclosing this feature. See page 7 of the Office Action. These sections have been reviewed, but Applicants find nothing in these sections that indicate that a printer key hash is obtained from a "test page" printed by a printer, and that the printer key hash is input into the computing device by a user-input means connected to the computing device.

Withdrawal of the rejection of Claim 23 is therefore respectfully requested.

An Information Disclosure Statement accompanies this Amendment. This Information Disclosure Statement is filed with a fee and with a certification under Rule 56(e) . Consideration of the art cited therein is respectfully requested.

In view of the foregoing, all claims herein are believed to be in condition for allowance, and such action is courteously solicited.

Applicants' undersigned attorney may be reached in our Costa Mesa, CA office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

Attorney for Applicants
Michael K. O'Neill
Registration No. 32,622

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3800
Facsimile: (212) 218-2200

CA_MAIN 131249v1